

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF NORTH CAROLINA
Civil Action No. 1:25-cv-00549-TDS-LPA

**WILLIAM MARSHALL, individually and on
behalf of all others similarly situated,**

Plaintiff,

-v-

**AHOLD DELHAIZE USA SERVICES, LLC
and HANNAFORD BROS. CO., LLC,**

Defendants.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

1. Plaintiff William Marshall (“Plaintiff”) brings this Class Action Complaint (“Complaint”) on behalf of Plaintiff and all others similarly situated against Defendant Ahold Delhaize USA Services, LLC (“Ahold”) and Hannaford Bros. Co., LLC (“Hannaford”) (together, “Defendants”) for failure to properly secure and safeguard Plaintiff’s and Class members’ personally identifiable information (“PII”) and protected health information (“PHI”) stored within Defendants’ information network and alleges as follows based upon information and belief, and the investigation of counsel, except as to the allegations specifically pertaining to Plaintiff, which are based on personal knowledge.

NATURE OF THE CASE

2. Entities that handle sensitive PII owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII to unauthorized persons—especially hackers with nefarious intentions — will result in harm to the affected individuals, including, but not limited to, the invasion of their private financial matters.

3. The harm resulting from a breach of private data manifests in a number of ways, including identity theft and financial fraud. The exposure of a person's PII through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and to take a number of additional prophylactic measures.

4. Defendants knowingly obtain sensitive employee PII and have a resulting duty to securely maintain such information in confidence.

5. As discussed in more detail below, Defendants breached their duty to protect the sensitive PII entrusted to them.

6. As such, Plaintiff brings this Class action on behalf of himself and other individuals whose PII was accessed and exposed to unauthorized third parties during a data breach of the Defendants' system between November 5th and 6th of 2024, which was announced when Defendants began providing notices on or about June 26, 2025 ("Data Breach").

7. The Data Breach impacted over 2.24 million individuals, and involved unauthorized access to internal business systems, including a file repository. This resulted in the exposure of PII and PHI.

8. Ahold is a support services provider for several major grocery brands, including Food Lion, Giant Food, The GIANT Company, Hannaford, and Stop & Shop.

9. The Data Breach occurred when an unauthorized third party gained access to files from an internal file repository between November 5 and 6, 2024.

10. The data exposed in the Data Breach included names, contact information, dates of birth, government-issued identification numbers (such as Social Security numbers, passport numbers, and driver's license numbers), financial account information (such as bank account number), health and medical information (such as workers' compensation information and medical information contained in employment records) and employment-related information, as Defendants reported to the Attorneys General of Maine, California, and Montana.¹

11. As a direct and proximate result of Defendants' inadequate data security, and their breach of their duty to handle PII and PHI with reasonable care, Plaintiff's PII and PHI have been accessed by hackers, potentially posted on the dark web, and exposed to an untold number of unauthorized individuals.

12. Plaintiff is now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of his health privacy, and similar forms of criminal mischief, and such risk may last for the rest of his life. Consequently, Plaintiff must devote substantially more time, money, and energy to protect himself, to the extent possible, from these crimes.

13. Plaintiff, on behalf of himself and others similarly situated, brings claims for negligence, negligence *per se*, breach of fiduciary duty, unjust enrichment, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

¹ See https://oag.ca.gov/system/files/Sample_Individual_Notification.pdf (last accessed June 27, 2025); see also, <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/b17963fc-3806-430e-b28e-bac47eb73a8b.html> (last accessed June 27, 2025); see also <https://dojmt.gov/wp-content/uploads/2025/06/Consumer-notification-letter-8.pdf> (last accessed June 27, 2025).

14. To recover from Defendants for their sustained, ongoing, and future harms, Plaintiff and Class members seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Defendants to: 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PII and PHI possessed by Defendants; and 3) provide, at Defendants' own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

15. Plaintiff William Marshall ("Marshall") is an adult individual and, at all relevant times herein, has been a resident and citizen of Maine residing in Cumberland County, where he intends to remain. Shortly after June 26, 2025, Plaintiff received a Notice of Data Breach from Defendant Ahold dated June 26, 2025 ("Notice").²

16. Defendant Ahold Delhaize USA Services LLC ("Ahold") is the services provider for grocery stores in the United States owned by non-party Koninklijke Ahold Delhaize N.V. a/k/a Royal Ahold Delhaize ("Ahold Delhaize"),³ an international retailing group based in the Netherlands and primarily active in the United States and Europe.

17. Ahold is a Delaware limited liability company with its principal office located at 2110 Executive Drive Salisbury, North Carolina 28147.⁴

² See **Exhibit A** hereto.

³ See <https://www.claimdepot.com/data-breach/ahold-delhaize-usa#:~:text=Ahold%20Delhaize%20USA%20Services%2C%20LLC,BI%2DLO%2C%20Inc.&ext=Bradlees%2C%20Inc.,Bruno's%20Supermarkets%2C%20Inc.&text=Mayfair%20Super%20Markets%2C%20Inc.&text=Purity%20Supreme%2C%20Inc.&text=Ahold%20Delhaize%20USA%2C%20Inc.&text=Ahold%20Information%20Services%2C%20Inc.> (last accessed June 27, 2025).

⁴ See <https://corp.sec.state.ma.us/CorpWeb/CorpSearch/CorpSummary.aspx?sysvalue=XwBqhxQiG9yOFgW7OIbbHLOrfNXjUv06u0ZZPtiREVs-> (last accessed June 27, 2025).

18. Ahold Delhaize's strong local brands in the United States are well known and popular with customers. Supermarkets are the core of the Ahold Delhaize's business. In the United States, Ahold Delhaize subsidiaries operate supermarkets under the Food Lion, Hannaford, Stop & Shop, Giant, and Martin's brands.⁵

19. Defendant Hannaford Bros. Co., LLC ("Hannaford") is a Maine limited liability company with its headquarters and principal place of business at 145 Pleasant Hill Road, Scarborough, Maine 04074.

20. Upon information and belief, Defendant Ahold is owned by Ahold Delhaize, the Netherlands parent company of Defendant Ahold.

21. Upon information and belief, Defendant Hannaford is a subsidiary of Ahold Delhaize, the Netherlands parent company of Defendant Ahold.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this class action exceeds \$5,000,000, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than North Carolina and/or the Netherlands, including Plaintiff, who is a citizen of the State of Maine, as, upon information and belief, Defendant Ahold, a limited liability company whose citizenship is determined by its members, is owned by Ahold Delhaize, the Netherlands parent company of Defendant Ahold; and upon information and belief, Defendant Hannaford is a subsidiary Ahold Delhaize, the Netherlands parent company of Defendant Ahold, and/or a subsidiary of Defendant Ahold.

⁵ See https://www.sec.gov/Archives/edgar/data/869425/000119312517095046/d358563d20f.htm#tx358563_5 (last accessed June 27, 2025).

23. This Court has personal jurisdiction over Defendants as they have substantial contacts with this District and transact business in this District.

24. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendants are deemed to reside in this District because they are subject to the Court's personal jurisdiction with respect to this action, a substantial part of the events giving rise to the claims herein occurred in this District, and Defendants regularly conduct business in this District.

FACTUAL BACKGROUND

A. Defendants and the Services they Provide

25. Defendants receive and handle PII and PHI, which includes, *inter alia*, grocery store employees' full names, addresses, Social Security numbers, driver's license or state ID numbers, financial account and payment information, and claims and health information.

26. Plaintiff was an Ahold employee and entrusted his information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

27. By obtaining, collecting, and storing Plaintiff's PII and PHI, Defendants assumed legal and equitable duties and knew or should have known that Defendants were responsible for protecting Plaintiff's PII and PHI from unauthorized disclosure.

28. Upon information and belief, Defendants fund their data security measures entirely from their general revenue, including payments made by or on behalf of Plaintiff and the Class members to entities that retain Defendants.

B. Defendants Knew the Risks of Storing Valuable PII and the Foreseeable Harm

29. At all relevant times, Defendants knew they were storing sensitive PII and PHI and that, as a result, their systems would be an attractive target for cybercriminals.

30. Defendants also knew that a breach of their systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI were compromised, as well as intrusion into their highly private information.

31. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.

32. For example, in 2023, the number of data compromises in the United States stood at 3,205 cases, affecting over 353 million individuals.⁶

33. The type and breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendants employees especially vulnerable to identity theft, tax fraud, medical fraud, credit, and bank fraud, and more.

34. PII is a valuable property right⁷ and their value is measurable. American companies are estimated to have spent over \$19 billion on acquiring personal data of consumers in 2018.⁸ It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the “cyber black-market,” or the “dark web,” for many years.

35. As a result of their real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in

⁶ See <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/> (last accessed June 20, 2025).

⁷ See https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data (“The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible”) (last accessed June 20, 2025).

⁸ See <https://www.iab.com/news/2018-state-of-data-report/> (last accessed June 20, 2025).

the Data Breach, can be aggregated, and becomes more valuable to thieves and more damaging to victims.

36. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: “[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.”⁹

37. Even if stolen PII does not include financial or payment card account information, which does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

38. Based on the value of their employees’ PII and PHI to cybercriminals and cybercriminals’ propensity to target businesses, Defendants certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

C. Defendants Breached their Duty to Protect their Employee’s PII and PHI

39. On or about June 26, 2025, Defendants announced that they experienced a security incident that, “[g]iven the nature of the file repository, the files that may have been affected contained different types of personal information such as name, contact information (for example,

⁹ See United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: <https://www.gao.gov/new.items/d07737.pdf> (last accessed June 15, 2025).

postal and email address and telephone number), date of birth, government-issued identification numbers (for example, Social Security, passport and driver's license numbers), financial account information (for example, bank account number), health information (for example, workers' compensation information and medical information contained in employment records), and employment-related information [and that] [t]he types of impacted information vary by affected individual.”¹⁰

40. Defendants disclosed on June 26, 2025 that “[u]pon detection last November, we began taking steps to assess and contain the issue, including working with external cybersecurity experts to investigate and secure the affected systems [and that] [w]e take this issue extremely seriously and will continue to take actions to further protect our systems.”¹¹

41. Like Plaintiff Marshall, other Class members received similar untimely notices of the Data Breach.

42. The Data Breach occurred as a direct result of Defendants' failure to implement and follow basic security procedures to protect their customers' and employees' PII and PHI.

43. The injury from the Data Breach is worsened due to Defendants' belated disclosure.

D. FTC Guidelines Prohibit Defendants from Engaging in Unfair or Deceptive Acts or Practices

44. Defendants are prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 (“FTC Act”) from engaging in “unfair or deceptive acts or practices in or affecting commerce.” The Federal Trade Commission (“FTC”) has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an “unfair practice” in violation of the FTC Act.

¹⁰ <https://dojmt.gov/wp-content/uploads/2025/06/Consumer-notification-letter-8.pdf> (last accessed June 27, 2025).

¹¹ *Id.*

45. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

46. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.¹²

47. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.¹³

48. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

49. Defendants failed to properly implement basic data security practices.

50. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

¹² See <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business> (last accessed June 20, 2025).

¹³ *Id.*

51. Defendants were at all times fully aware of their obligations to protect customers' PII and PHI. Defendants are also aware of the significant repercussions that would result from their failure to do so.

E. Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

52. Cyberattacks and data breaches at companies that store PII and PHI are especially problematic because they can negatively impact on the overall daily lives of individuals affected by the attack.

53. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."¹⁴

54. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate

¹⁴ See <https://www.gao.gov/products/gao-07-737> (last accessed June 20, 2025).

individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

55. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, receive medical treatment, open new utility accounts, and incur charges and credit in a person's name.

56. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing freezes on their credit, and correcting their credit reports.¹⁵

57. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. Personal information is valuable to identity thieves, and if they can get access to it, they will use it to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

58. Identity thieves can also use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

¹⁵ See <https://www.identitytheft.gov/Steps> (last accessed June 20, 2025).

59. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.

60. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII on the black market for the purpose of target-marketing their products and services to the physical maladies of data breach victims themselves.

61. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the PII stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiff.

62. As discussed above, PII is such a valuable commodity to identity thieves, and once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

63. Social Security numbers are particularly sensitive pieces of personal information. For instance, with a stolen Social Security number, which is only one subset of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits. Identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may be undetected until debt collection calls commence months, or even years later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply

for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected because one was already filed on their behalf.

64. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as the credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.

65. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like Defendants is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market.

66. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years later. As with income tax returns, an individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notified the individual's employer of the suspected fraud.

67. Cybercriminals can post stolen PII on the cyber black market for years following a data breach, thereby making such information publicly available. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.

68. It is within this context that Plaintiff must now live with the knowledge that Plaintiff's PII is forever in cyberspace and was taken by people willing to use the information for

any number of improper purposes and scams, including making the information available for sale on the black market.

69. Plaintiff must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on Plaintiff's everyday life, including purchasing identity theft and credit monitoring services every year for the rest of Plaintiff's life, placing "freezes" and "alerts" with credit reporting agencies, contacting his financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

70. Moreover, Plaintiff and Class members have an interest in ensuring that their PII, which remains in the possession of Defendants, are protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendants have shown themselves to be wholly incapable of protecting Plaintiff's PII.

71. Plaintiff and Class members also have an interest in ensuring that their personal information that was provided to Defendants is removed from Defendants' unencrypted files.

F. Plaintiff and the Class Suffered Damages

Facts Relevant to Plaintiff

72. Plaintiff is a former employee of Defendants.

73. Plaintiff was employed at a Hannaford grocery store in Maine from June of 2020 through May of 2023.

74. As a condition of his employment with Defendants, he was required to provide his PHI and PII to Defendants.

75. Defendants, upon information and belief, retained Plaintiff's PII and PHI in their systems at the time of the Data Breach.

76. Shortly after June 26, 2025, Plaintiff received a Notice of Data Breach from Defendant Ahold dated June 26, 2025.¹⁶

77. As alleged (*see ¶ 39, supra*), the Notice at-large to the Attorneys General and the Notice specifically received by Plaintiff Marshall state that, “[g]iven the nature of the file repository [maintained by Defendants related to Plaintiff and Class members], the files that may have been affected contained different types of personal information such as name, contact information (for example, postal and email address and telephone number), date of birth, government-issued identification numbers (for example, Social Security, passport and driver's license numbers), financial account information (for example, bank account number), health information (for example, workers' compensation information and medical information contained in employment records), and employment-related information [and that] [t]he types of impacted information vary by affected individual.”¹⁷

78. Defendants received Plaintiff's PII and PHI in connection with and as a condition of his employment. In requesting and maintaining Plaintiff's PII and PHI for business purposes, Defendants expressly and impliedly promised, and undertook a duty, to act reasonably in their handling of Plaintiff's and Class members' PII and PHI. Defendants did not, however, take proper care of Plaintiff's and Class members' PII and PHI, leading to their exposure to and exfiltration by cybercriminals as a direct result of Defendants' inadequate security measures.

¹⁶ See **Exhibit 1** hereto.

¹⁷ *Id.*

79. Upon receiving Notice, Plaintiff spent time reviewing his credit reports, reviewing various credit alerts received by text and email, checking his financial information, and dealing with increased spam text messages and emails.

80. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

81. Plaintiff has experienced anxiety and increased concerns arising from the fact that his PII has been or will be misused and from the loss of his privacy.

82. The risk is not hypothetical, as cybercriminals intentionally stole the data, misused it, threatened to publish, or have published it on the dark web, and the sensitive information, including names and Social Security numbers, which is the type of PII used to perpetrate identity theft or fraud.

83. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of his PII and PHI—forms of intangible property that he entrusted to Defendants, which was compromised in and because of the Data Breach.

84. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

85. Plaintiff has a continuing interest in ensuring that his PII and PHI, which remain in Defendants' possession, are protected and safeguarded from future breaches.

Plaintiff's And Class Members' Damages

86. For the reasons mentioned above, Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiff and Class members significant injuries and harm in several ways.

Plaintiff and Class members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them. Plaintiff and Class members have taken or will be forced to take these measures in order to mitigate their potential damages as a result of the Data Breach.

87. Once PII is exposed, there is little that can be done to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendants' conduct.

88. As a result of Defendants' failures, Plaintiff and Class members are also at substantial and certainly impending increased risk of suffering identity theft and fraud or misuse of their PII.

89. Plaintiff is also at a continued risk because Plaintiff's information remains in Defendants' computer systems, which have already been shown to be susceptible to compromise and attack and are subject to further attacks so long as Defendants fail to undertake the necessary and appropriate security and training measures to protect their employees' and former employees' PII.

90. In addition, Plaintiff and Class members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

CLASS ALLEGATIONS

91. Plaintiff brings all counts, as set forth below, individually and as a Class action, pursuant to Fed. R. Civ. P. 23, on behalf of a Class defined as: **All individuals within the United States of America whose PII, PHI, and/or financial information was exposed to unauthorized third-parties as a result of the Data Breach experienced by Defendants** (“Class”).

92. Excluded from the Class are Defendants, their subsidiaries and affiliates, officers and directors, any entity in which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

93. This proposed Class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the Class definition in an amended pleading or when he moves for Class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

94. **Numerosity** – Fed. R. Civ. P. 23(a)(1): Plaintiff is informed and believes, and thereon alleges, that there are at minimum, over a thousand members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendants’ records, including but not limited to the files implicated in the Data Breach.

95. **Commonality** – Fed. R. Civ. P. 23(a)(2): This action involves questions of law and fact common to the Class. Such common questions include, but are not limited to:

- a. Whether Defendants have a duty to protect Plaintiff’s and Class members’ PII;
- b. Whether Defendants were negligent in collecting and storing Plaintiff’s and Class members’ PII, and breached their duties thereby;

- c. Whether Defendants breached their fiduciary duty to Plaintiff and the Class;
- d. Whether Defendants breached their duty of confidence to Plaintiff and the Class;
- e. Whether Defendants violated their own Privacy Practices;
- f. Whether Defendants were unjustly enriched;
- g. Whether Plaintiff and Class members are entitled to damages as a result of Defendants' wrongful conduct; and
- h. Whether Plaintiff and Class members are entitled to restitution as a result of Defendants' wrongful conduct.

96. **Typicality** – Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class all had information stored in Defendants' system(s), each having their PII and/or PHI exposed and/or accessed by an unauthorized third party.

97. **Adequacy of Representation** – Fed. R. Civ. P. 23(a)(3): Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex Class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

98. **Injunctive Relief** – Fed. R. Civ. P. 23(b)(2): Defendants have acted and/or refused to act on grounds that apply generally to the Class therefore making injunctive and/or declarative relief appropriate with respect to the Class under 23(b)(2).

99. **Superiority** – Fed. R. Civ. P. 23(b)(3): A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

100. Defendants have acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

101. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendants failed to timely and adequately notify the public of the Data Breach;
- b. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

- c. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;
- e. Whether Defendants failed to take commercially reasonable steps to safeguard employees' PII; and
- f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

102. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to Class members' names and addresses affected by the Data Breach.

FIRST CAUSE OF ACTION
NEGLIGENCE

103. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

104. Plaintiff brings this claim individually and on behalf of the Class.

105. Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII and PHI in their possession, custody, and control.

106. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

107. Defendants have a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendants. By collecting and storing valuable

PII that is routinely targeted by criminals for unauthorized access, Defendants were obligated to act with reasonable care to protect against these foreseeable threats.

108. Defendants breached the duties owed to Plaintiff and Class members and thus were negligent. As a result of a successful attack directed towards Defendants that compromised Plaintiff's and Class members' PII, Defendants breached their duties through the following errors and omissions that allowed the Data Breach to occur:

- a. mismanaging their system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII;
- b. mishandling their data security by failing to assess the sufficiency of their safeguards in place to control these risks;
- c. failing to design and implement information safeguards to control these risks;
- d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;
- e. failing to evaluate and adjust their information security program in light of the circumstances alleged herein;
- f. failing to detect the breach at the time it began or within a reasonable time thereafter;
- g. failing to follow their own privacy policies and practices published to their customers; and

h. failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII.

109. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class members, their PII would not have been compromised.

110. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have suffered injuries, including, but not limited to:

- a. Theft of their PII and PHI;
- b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII and PHI;
- c. Costs associated with purchasing credit monitoring and identity theft protection services;
- d. Lowered credit scores resulting from credit inquiries following fraudulent activities;
- e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;
- f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and PHI being placed in the hands of criminals;

- g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others;
- h. Continued risk of exposure to hackers and thieves of their PII and PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data; and
- i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

111. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*

112. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

113. Plaintiff brings this claim individually and on behalf of the Class.

114. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendants for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duty.

115. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of a data breach involving PII of their customers.

116. Plaintiff and members of the Class are consumers within the Class of persons Section 5 of the FTC Act was intended to protect.

117. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

118. The harm that has occurred as a result of Defendants' conduct is the type of harm that the FTC Act and Part 2 was intended to guard against.

119. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY

120. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

121. Plaintiff brings this claim individually and on behalf of the Class.

122. Plaintiff and Class members have an interest, both equitable and legal, in the PII and PHI about them that was conveyed to, collected by, and maintained by Defendants and that was ultimately accessed or compromised in the Data Breach.

123. As a recipient of its employees' PII and PHI, Defendants have a fiduciary relationship to Plaintiff and the Class members.

124. Because of that fiduciary relationship, Defendants were provided with and stored private and valuable PII and PHI related to Plaintiff and the Class. Plaintiff and the Class were entitled to expect their information would remain confidential while in Defendants' possession.

125. Defendants owed a fiduciary duty under common law to Plaintiff and Class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

126. As a result of the parties' fiduciary relationship, Defendants had an obligation to maintain the confidentiality of the information within Plaintiff's and the Class members' records.

127. Defendants had possession and knowledge of confidential PII and PHI of Plaintiff and Class members, information not generally known.

128. Plaintiff and Class members did not consent to nor authorize Defendants to release or disclose their PII and PHI to unknown criminal actors.

129. Defendants breached their fiduciary duties owed to Plaintiff and Class members by, among other things: mismanaging their system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; mishandling their data security by failing to assess the sufficiency of their safeguards in place to control these risks; failing to design and implement information safeguards to control these risks; failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; failing to evaluate and adjust their information security program in light of the circumstances alleged herein; failing to detect the breach at the time it began or within a reasonable time thereafter; failing to follow their own privacy policies and practices published to their customers and employees; and

failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII and PHI.

130. But for Defendants' wrongful breach of their fiduciary duties owed to Plaintiff and Class members, their PII would not have been compromised.

131. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have suffered injuries, including:

- a. Theft of their PII and PHI;
- b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII and PHI;
- c. Costs associated with purchasing credit monitoring and identity theft protection services;
- d. Lowered credit scores resulting from credit inquiries following fraudulent activities;
- e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;
- f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

- g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to with the mutual understanding that Defendants would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others;
- h. Continued risk of exposure to hackers and thieves of their PII and PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data; and
- i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

132. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT

133. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

134. Plaintiff brings this claim individually and on behalf of the Class.

135. Upon information and belief, Defendants fund their data security measures entirely from their general revenue, including payments made by or on behalf of Plaintiff and the Class members.

136. As such, a portion of the payments made by or on behalf of Plaintiff and the Class members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

137. Plaintiff and Class members conferred a benefit on Defendants by their employment. In exchange, Plaintiff and Class members should receive from Defendants the consideration of adequate protection in the subject of the transaction of their employment and have their PII/PHI protected with adequate data security.

138. Defendants knew that Plaintiff and Class members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the PII of Plaintiff and Class members for business purposes.

139. In particular, Defendants enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to increase their own profits at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize their own profits over the requisite security.

140. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class members, because Defendants failed to implement appropriate data management and security measures that are mandated by their common law and statutory duties.

141. Defendants failed to secure Plaintiff and Class members' PII and, therefore, did not provide full consideration for the benefit Plaintiff and Class members provided.

142. Defendants acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

143. If Plaintiff and Class members knew that Defendants had not reasonably secured their PII, they would not have agreed to have their information provided to Defendants.

144. Plaintiff and Class members have no adequate remedy at law.

145. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members have suffered injuries, including, but not limited to:

- a. Theft of their PII and PHI;
- b. Costs associated with purchasing credit monitoring and identity theft protection services;
- c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII and PHI;
- d. Lowered credit scores resulting from credit inquiries following fraudulent activities;
- e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;
- f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

- g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others;
- h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data; and
- i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

146. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm.

147. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them in their employment with Defendants.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT

148. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

149. Plaintiff brings this claim individually and on behalf of the Class.

150. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting

further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

151. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class members' PII and PHI, and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class members from future data breaches that compromise their PII and PHI. Plaintiff and the Class remain at imminent risk that additional compromises of their PII and PHI will occur in the future.

152. The Court should also issue prospective injunctive relief requiring Defendants to employ adequate security practices consistent with law and industry standards to protect consumers' PII and PHI.

153. Defendants still possess Plaintiff's and Class members' PII and PHI.

154. Defendants have made no announcement that it has changed their data storage or security practices relating to the storage of Plaintiff's and Class members' PII and PHI.

155. To Plaintiff's knowledge, Defendants have made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

156. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach of Defendants' networks. The risk of another such breach is real, immediate, and substantial.

157. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another data breach occurs in Defendants' systems, Plaintiff and Class members will likely continue to be subjected to

a heightened, substantial, imminent risk of fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

158. Issuance of the requested injunction will not compromise the public interest. On the contrary, such an injunction would benefit the public by preventing another data breach in Defendants' systems, thus eliminating the additional injuries that would result to Plaintiff and Class members, along with other consumers whose PII and PHI would be further compromised.

159. Pursuant to their authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendants implement and maintain reasonable security measures, including but not limited to the following:

- a. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;
- b. Engaging third-party security auditors and internal personnel to run automated security monitoring;
- c. Auditing, testing, and training their security personnel regarding any new or modified procedures;
- d. Purging, deleting, and destroying PII and PHI not necessary for their provisions of services in a reasonably secure manner;
- e. Conducting regular database scans and security checks; and

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

DEMAND FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, demands relief as follows:

- a) For an Order certifying this action as a Class action and appointing Plaintiff as a Class Representative and his counsel as Class Counsel;
- b) For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' PII and PHI, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;
- c) For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;
- d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;
- e) Ordering Defendants to pay for not less than three years of credit monitoring services for Plaintiff and the Class;
- f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- g) For an award of punitive damages, as allowable by law;

- h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- i) Pre- and post-judgment interest on any amounts awarded; and,
- j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded by Plaintiff on all claims so triable.

July 1, 2025

/s/ J. Matthew Norris

Matt Norris
NORRIS LAW FIRM PLLC
1776 Heritage Center Drive, Suite 204
Wake Forest, North Carolina 27587
Telephone: 919-981-4475
Facsimile: 919-926-1676
matt@lemonlawnc.com
NC Bar No. 37206

Rachele R. Byrd (*pro hac vice forthcoming*)
WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: 619-239-4599
byrd@whafh.com

Carl Malmstrom (*pro hac vice forthcoming*)
WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLC
111 W. Jackson Blvd., Suite 1700
Chicago, Illinois 60604
Telephone: 312-984-0000
malmstrom@whafh.com

James F. Woods (*pro hac vice forthcoming*)
Annie E. Causey (*pro hac vice forthcoming*)
WOODS LONERGAN
One Grand Central Place
60 East 42nd St., Suite 1410

New York, NY 10165
Telephone: 212-684-2500
jwoods@woodslaw.com
NY Bar No. 2302297
acausey@woodslaw.com

Jon Tostrud (*pro hac vice forthcoming*)
TOSTRUD LAW GROUP, PC
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: 310-278-2600
Facsimile: 310-278-2640
jtostrud@tostrudlaw.com

Erik Langeland (*pro hac vice forthcoming*)
ERIK H. LANGELAND, P.C.
733 Third Avenue, 16th Floor
New York, NY 10017
Telephone: 212-354-6270
elangeland@langelandlaw.com